UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of

Black iPhone 12; S/N: H4YM63CB0DXP, CURRENTLY LOCATED AT Sacramento Valley Internet Crimes Against Children Task Force located at 10151 Croydon Way, Sacramento, CA 95827

Case No. 2:24-sw-0356 CKD

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A, attached hereto and incorporated by reference.

located in the Eastern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2251(a);	Sexual exploitation of a child
18 U.S.C. § 2252(a); 2252A(a)	Receipt and possession of child pornography
18 U.S.C. § 2422(b); 2423(a)	Coercion and enticement; transportation of a minor for unlawful sex

The application is based on these facts:

SEE AFFIDAVIT, attached hereto and incorporated by reference.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice [ ] days (give exact ending date if more than 30 days: [ ]) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/

Applicant's signature

Caitlin Thomas, Special Agent, HSI

Printed name and title

Submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3)

Date: April 5, 2024 at 11:16 am

Carolyn K. Delaney

Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, U.S. Magistrate Judge

PHILLIP A. TALBERT
Acting United States Attorney
ROGER YANG
Assistant United States Attorney
501 I Street, Suite 10-100
Sacramento, CA 95814
Telephone: (916) 554-2700
Facsimile: (916) 554-2900

Attorneys for Plaintiff
United States of America

IN THE UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF CALIFORNIA

In the Matter of the Search of: Black iPhone 12; S/N: H4YM63CB0DXP	CASE NO. AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH DEVICES

1. I, Caitlin Thomas, being first duly sworn, hereby depose and state as follows:

I. INTRODUCTION AND AGENT BACKGROUND

2. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

1. I am a Special Agent ("SA") with Homeland Security Investigations ("HSI") and have been so employed since April 2019. I trained at the Federal Law Enforcement Training Center and have gained experience through everyday work conducting these types of investigations. I have received training in the areas of child sexual abuse material ("CSAM") and have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to the sexual exploitation of children, child

pornography, coercion and enticement, and transportation of minors, including violations of 18 U.S.C. §§ 2251, 2252, and 2252A, as well as §§ 2422 and 2423, and I am authorized by law to request a search warrant. I have participated in investigating federal criminal violations related to high technology or cybercrime, and CSAM. Additionally, I am a member of the Sacramento Valley Internet Crimes Against Children ("ICAC") Task Force. As an SA in the Sacramento Field Office and ICAC Task Force, I frequently participate in search warrant executions involving child exploitation and pornography cases. In June 2022, I attended the National Law Enforcement Training on Child Exploitation which offered classes ranging from investigative techniques and digital forensics. Moreover, I work closely with HSI forensic examiners throughout these investigations and prosecutions.

2. I have conducted and participated in criminal investigations for violations of federal and state laws including narcotics trafficking, child sexual exploitation, money laundering, and other organized criminal activity. I have prepared, executed, and assisted in numerous search and arrest warrants. I have also conducted and participated in criminal and administrative interviews of witnesses and suspects. I am familiar with the formal methods of child exploitation investigations, including electronic surveillance, visual surveillance, general questioning of witnesses, search warrants, and the use of undercover agents. I have participated in investigations of possession, distribution, receipt, and production of CSAM.

3. This affidavit is submitted in support of a search warrant for evidence, contraband, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, as well as §§ 2422 and 2423. As set forth below, there is probable cause to believe that such items, as set forth in Attachment B, attached hereto and incorporated herein by reference, will be found at the locations described in Attachment A, which is also attached hereto and incorporated herein by reference.

4. The facts set forth in this affidavit are based on information provided to me from a law enforcement officer who acted in an undercover capacity; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this affidavit is submitted for the limited purpose of establishing probable cause in support of an application for a search warrant, it does not set forth each and every fact that I or others have learned during the course

of this investigation. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

II. APPLICABLE LAW

5. 18 U.S.C. § 2251(a) prohibits any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in any sexually explicit conduct for the purpose of producing any explicit depiction of such conduct or for the purpose of transmitting a live depiction of such conduct. 18 U.S.C. § 2251(e) states that attempts to sexually exploit minors are punished in the same manner as the substantive offense.

6. 18 U.S.C. § 2252(a)(2) prohibits the knowing receipt or distribution, by computer or mail, of any visual depiction of minors engaging in sexually explicit conduct, if the visual depiction has been mailed, shipped, or transported in interstate or foreign commerce, or if it contains materials that have been so mailed, shipped, or transported, by any means, including by computer.

7. 18 U.S.C. § 2252(a)(4)(B) prohibits the possession of one or more matters that contain visual depictions of minors engaged in sexually explicit conduct, and that have been mailed, shipped, or transported in interstate or foreign commerce, or if it contains materials that have been so mailed, shipped, or transported, by any means, including by computer.

8. 18 U.S.C. § 2422(b) prohibits a person from knowingly persuading, inducing, enticing, or coercing any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense.

9. 18 U.S.C. § 2423(a) prohibits a person from knowingly transporting any individual who has not attained the age of 18 years in interstate or foreign commerce with intent that the individual engage in prostitution or in any criminal sexual activity. Attempts to transport a minor with the intent that the minor engage in illegal sexual activity are punished in the same manner under § 2423(e).

III. IDENTIFICATION OF THE DEVICES TO BE EXAMINED

10. The following item to be searched was seized from Joshua David PRICE on March 29, 2024, following his arrest during an undercover chat operation: Black iPhone 12; S/N: H4YM63CB0DXP, hereinafter the "Device." The Device is currently located in the evidence room at the Sacramento Valley Internet Crimes Against Children Task Force located at 10151 Croydon Way,

Sacramento, CA 95827.

11. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

IV. PROBABLE CAUSE

12. On or about March 19, 2024, a Placer County Sheriff's Office ("PCSO") Detective, while acting in an undercover capacity, assumed the persona of a 13-year-old female on various mobile-based chat applications. This Detective (hereinafter referred to as Undercover Agent ("UCA") received a private message on an anonymous chatting application, Whisper, from a user who was later identified as Joshua David PRICE. On multiple occasions and across different mobile-based chatting applications, PRICE was made aware of the age of the UCA's persona. On April 4, 2024, your affiant reviewed screenshots of these conversations that took place on March 19, 2024; the conversation is as follows:

> The UCA posted on Whisper,[1] "I hate class." Another Whisper user, "Aluminum_Nature," initiated the conversation, as follows:
>
> *Aluminum_Nature: What class*
> UCA: It was math
> UCA: I'm in Spanish now
> *Aluminum_Nature: No fuxking [sic] kidding?*
> UCA: Yea you want to text me?
> *Aluminum_Nature: How young are you*
> UCA: I'm 13
> UCA: U?
> *Aluminum_Nature: I'm 34 is that okay?*
> UCA: Yeah
> UCA: Where u from
> *Aluminum_Nature: I'm on the west coast you?*
> UCA: same I'm in Roseville
> UCA: I'm Olivia
> *Aluminum_Nature: I'm Josh got anything other than this to talk on?*
> *Aluminum_Nature: Yes plz*
> UCA: 530-718-3236
> *Aluminum_Nature: Your parents don't monitor it do they?*
> UCA: no I'm almost 14
> UCA: My parents are split up
> *Aluminum_Nature: That sucks will ill be your friend an more if you want I texted you my*

[1] Whisper, a free mobile application, is a form of anonymous social networking allowing users to post and share photo and video messages anonymously. The posts, called "whispers," consist of text that is superimposed over an image that is chosen by the user.

numbers 661-376-1141
UCA: ok
UCA: Nothing has come yet

13. On or about March 19, 2024, the Sacramento Valley Internet Crimes Against Children ("ICAC") Task Force Detectives looked up the cellphone number, "(661) 376-1141," in Law Enforcement Databases and observed that it was associated to Joshua David PRICE; DOB: 10/17/1989; Transient in Sacramento, CA. Other law enforcement databases showed that PRICE was on searchable parole, and was subject to sex offender parole conditions, including search and seizure of devices, a requirement to surrender passcodes and passwords, and no contact with minors.

14. Following PRICE and the UCA exchanging numbers, the conversation transferred off the Whisper application to text messaging. On April 4, 2024, your affiant reviewed a PDF report of the text messages that took place between PRICE and the UCA during March 19, 2024, and March 29, 2024. During review, your affiant noted the following messages:

On March 19, 2024, at 11:16:32 AM, PRICE sent the following message:

"I'm just leary [sic] and worried not cause of your age idgaf bout that but cause sadly I've been caught up talking to a 16 yr old once I hope that doesn't scare you off..."

Later that same day at 11:21:42 AM, PRICE sent the following message:

"Mhm ngl I've done it 3 times only with 3 younger women I am ngl my first was 16, second was 14 and virgin, third was 14."

Later that same day at 04:39:11 PM, PRICE sent the following message:

"No liv my only vice that aren't quite legal but I only do one of those at a time and if this first meeting goes good hopefully you'll be the last one."

On March 20, 2024, at 03:06:27 PM, PRICE sent the following message:

"You sitting on my lap n I'm knocking at your lady parts you start grinding next thing you know you can't breathe on your back going harder Josh harder."

On March 21, 2024, PRICE told the UCA that he is on an ankle monitor and had been to prison. Also, on March 21, 2024, at 08:16:03 PM, PRICE sent the following message:

"Ngl I want to cream all over your face n take a picture"

On March 28, 2024, the following conversation took place:

UCA at 09:28:22 PM: You going to sleep to?

PRICE at 09:28:37 PM: Not yet I'm excited now

UCA at 09:29:04 PM: Hope you save some excitement for me

UCA at 09:29:24 PM: lol

PRICE at 09:29:30 PM: I'm cumming till in your mouth

UCA at 09:29:44 PM: Promise?

PRICE at 09:29:58 PM: Promise n I wanna film it

15. On March 29, 2024, the Sacramento Sexual Assault Felony Enforcement ("SAFE") task force, who registers convicted sex offenders within the city of Sacramento and the unincorporated area of Sacramento County including the city of Rancho Cordova, began closely monitoring the location of PRICE to determine if he was moving towards the designated meet location, a Starbucks located at 2620 Gateway Oaks Drive, Sacramento, CA 95833. At approximately 1200 hours, your affiant observed the tracking information associated to PRICE's ankle monitor and noted that he was tracked walking around the Starbucks and shopping center.

16. At approximately 1215 hours, PRICE was arrested on Gateway Oaks walking away from the Starbucks towards the residences. PRICE was subsequently transported to the Fairfield Inn & Suites located at 2730 El Centro Rd, Sacramento, CA 95833 to be interviewed.

17. During the interview, PRICE gave consent to search his phone at approximately 1331 hours. PRICE also acknowledged that he was on parole, and that his conditions of parole allowed law enforcement to seize and search his phone without a warrant, obtain passcodes and passwords from him, and that he was not supposed to be contacting minors on social media.

18. Following the interview, your affiant reviewed PRICE's phone and observed a text conversation with what appears to be a minor female. Within the text messages, your affiant observed the following:

On March 28, 2024, at approximately 1506 hours, PRICE received a close-up image of the minor's vagina with her fingers pulling the vagina back slightly; there was no visible pubic hair. At approximately 1508 hours, PRICE sent a 35 second video of what appears to be himself masturbating

and ejaculating while laying on a bed. Following the video, PRICE sent a text at 1510 hours stating, "You think you would've been able to swallow it all?" Later in the conversation, PRICE sent a text at 1557 hours stating, "Imma fuck you so hard you won't be able to walk unless you say your pussy is not ugly." Shortly thereafter, at 1559 hours, the minor victim sent PRICE a photo depicting a close-up of her vagina with two fingers placed near the top of the vagina; there is no visible pubic hair. In response to this photo, PRICE states, "I wanna suck on them and bite them and make you moan." Following this text, the minor victim sent another photo at 1600 hours, with a text after which reads, "my hymen." This photo depicts what appears to be the same female using her index and middle finger to spread the labias of her vagina apart. In response to this photo, PRICE states, "I wanna pop it."

V. TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a) "Bulletin Board" means an Internet-based website that is either secured (accessible with a password) or unsecured and provides members with the ability to view postings by other members and make postings themselves. Postings can contain text messages, still images, video images, or web addresses that direct other members to specific content the poster wishes. Bulletin boards are also referred to as "internet forums" or "message boards." A "post" or "posting" is a single message posted by a user. Users of a bulletin board may post messages in reply to a post. A message "thread," often labeled a "topic," refers to a linked series of posts and reply messages. Message threads or topics often contain a title, which is generally selected by the user who posted the first message of the thread. Bulletin boards often also provide the ability for members to communicate on a one-to-one basis through "private messages." Private messages are similar to e-mail messages that are sent between two members of a bulletin board. They are accessible only by the users who sent/received such a message, or by the bulletin board administrator.

b) "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation.

This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

c) "Chat room," as used herein, refers to the ability of individuals to meet in one location on the Internet in order to communicate electronically in real-time to other individuals. Individuals may also have the ability to transmit electronic files to other individuals within the chat room.

d) "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

e) "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

f) "Cloud storage," as used herein, is a form of digital data storage in which the digital data is stored on remote servers hosted by a third party (as opposed to, for example, on a user's computer or other local storage device) and is made available to users over a network, typically the Internet.

g) "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. See 18 U.S.C. § 1030(e)(1).

h) "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices

(including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

i) "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

j) The "Domain Name System" or "DNS" is system that translates readable Internet domain names such as www.justice.gov into the numerical IP addresses of the computer server that hosts the website.

k) "Encryption" is the process of converting data into a code in order to prevent unauthorized access to the data.

l) A "hidden service," also known as an "onion service," is website or other web service that is accessible only to users operating within the Tor network.

m) "Hyperlink" refers to an item on a web page which, when selected, transfers the user directly to another location in a hypertext document or to some other web page.

n) The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

o) "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

p) An "Internet Protocol address" or "IP address," as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers ("ISPs") control a range of IP addresses. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

q) "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

r) "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

s) "Remote computing service," as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

t) "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

u) A "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, "thumb," "jump," or "flash" drives, CD-

ROMs, and other magnetic or optical media.

v) The "Tor network" is a computer network available to Internet users that is designed specifically to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of relay computers, along a randomly assigned path known as a "circuit."

w) "URL" is an abbreviation for Uniform Resource Locator and is another name for a web address. URLs are made of letters, numbers, and other symbols in a standard form. People use them on computers by clicking a pre-prepared link or typing or copying and pasting one into a web browser to make the computer fetch and show some specific resource (usually a web page) from another computer (web server) on the Internet.

x) "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

y) A "Website" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

VI. ELECTRONIC STORAGE AND FORENSIC ANALYSIS

20. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

21. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

a) Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded

onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b) Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space-that is, in space on the storage medium that is not currently being used by an active file-for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c) Wholly apart from user-generated files, computer storage media-in particular, computers' internal hard drives-contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d) Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

22. Forensic evidence. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Devices were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Devices because:

a) Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on

the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b) Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c) A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d) The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e) Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

24. Manner of execution. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical

intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

VII. CONCLUSION

25. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits, and instrumentalities of these offenses, more fully described in Attachment B, are located in the devices described in Attachment A. I respectfully request that this Court issue a search warrant for the devices described in Attachment A, authorizing the seizure and search of the items described in Attachment B.

26. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab; digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the Devices. Unless otherwise ordered by the Court, the return will not include evidence later examined by a forensic analyst.

Respectfully submitted,

/s/
Caitlin Thomas
Special Agent
Homeland Security Investigations (HSI)

Affidavit submitted by email and attested to me as true and accurate by telephone consistent with Fed. R. Crim. P. 4.1 and 41(d)(3)

April 5, 2024

The Honorable Carolyn K. Delaney
UNITED STATES MAGISTRATE JUDGE

/s/ ROGER YANG
Approved as to form by AUSA ROGER YANG

ATTACHMENT A

The property to be searched is a black iPhone 12, S/N: H4YM63CB0DXP hereinafter the "Device." The Device is currently located at Sacramento Valley Internet Crimes Against Children Task Force located at 10151 Croydon Way, Sacramento, CA 95827.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

The items to be seized are the following materials, which constitute evidence of the commission of a criminal offense, contraband, instrumentalities, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, and 2422(b) and 2423:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence relating to use of Tor, the Dark Web, or other alternatives to the traditional Internet;

f. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

g. evidence of communications with minors relating to transportation and sexual activity; with minors' relatives, with PRICE's friends, siblings, and relatives relating to transportation of minors or sexual activity with minors, and evidence of travel arrangements involving minors;

h. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

i. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

j. evidence of the times the COMPUTER was used;

k. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

l. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

m. records of or information about Internet Protocol addresses used by the COMPUTER;

n. evidence concerning the use of digital cameras, recording devices, and other means of creating visual depictions of minors engaged in sexual conduct;

o. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

p. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

a. Records, information, and items relating to violations of the statutes described above including:

b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

c. Records and information about payments or transfers, including Bitcoin or other cryptocurrencies, relating to the sexual exploitation of children;

d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

5. Google search terms or Google Maps directions to designated meet location(s);

6. Google search of Undercover Agent ("UCA") phone number or other user names or user accounts of potential minors;
7. Reverse image searches of UCA decoy pictures or pictures of possible minors;
8. Statements regarding awareness of parole conditions;

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.

AO 93 (Rev. 11/13) Search and Seizure Warrant

UNITED STATES DISTRICT COURT

for the

Eastern District of California

In the Matter of the Search of Black iPhone 12; S/N: H4YM63CB0DXP, CURRENTLY LOCATED AT Sacramento Valley Internet Crimes Against Children Task Force located at 10151 Croydon Way, Sacramento, CA 95827	)	Case No. 2:24-sw-0356 CKD

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of California

(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A, attached hereto and incorporated by reference.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B, attached hereto and incorporated by reference.

YOU ARE COMMANDED to execute this warrant on or before April 19, 2024 *(not to exceed 14 days)*

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☑ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to: any authorized U.S. Magistrate Judge in the Eastern District of California.

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

☐ for ____ days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of ____.

Date and time issued: April 5, 2024 at 11:16 am

Carolyn K. Delaney

Judge's signature

City and state: Sacramento, California

Carolyn K. Delaney, U.S. Magistrate Judge

Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2) (modified)

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I swear that this inventory is a true and detailed account of the person or property taken by me on the warrant.

Subscribed, sworn to, and returned before me this date.

Signature of Judge

Date

ATTACHMENT A

The property to be searched is a black iPhone 12, S/N: H4YM63CB0DXP hereinafter the "Device." The Device is currently located at Sacramento Valley Internet Crimes Against Children Task Force located at 10151 Croydon Way, Sacramento, CA 95827.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

The items to be seized are the following materials, which constitute evidence of the commission of a criminal offense, contraband, instrumentalities, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A, and 2422(b) and 2423:

1. Computers or storage media used as a means to commit the violations described above.
2. For any computer or storage medium whose seizure is otherwise authorized by this warrant, and any computer or storage medium that contains or in which are stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
    a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
    b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
    c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to the crime(s) under investigation and to the computer user;

e. evidence relating to use of Tor, the Dark Web, or other alternatives to the traditional Internet;

f. evidence indicating the computer user's knowledge and/or intent as it relates to the crime(s) under investigation;

g. evidence of communications with minors relating to transportation and sexual activity; with minors' relatives, with PRICE's friends, siblings, and relatives relating to transportation of minors or sexual activity with minors, and evidence of travel arrangements involving minors;

h. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

i. evidence of programs (and associated data) that are designed to eliminate data from the COMPUTER;

j. evidence of the times the COMPUTER was used;

k. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

l. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

m. records of or information about Internet Protocol addresses used by the COMPUTER;

n. evidence concerning the use of digital cameras, recording devices, and other means of creating visual depictions of minors engaged in sexual conduct;

o. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

p. contextual information necessary to understand the evidence described in this attachment.

3. Routers, modems, and network equipment used to connect computers to the Internet.

4. Child pornography, as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaging in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2), and child erotica.

a. Records, information, and items relating to violations of the statutes described above including:

b. Records and information relating to the identity or location of the persons suspected of violating the statutes described above;

c. Records and information about payments or transfers, including Bitcoin or other cryptocurrencies, relating to the sexual exploitation of children;

d. Records and information relating to sexual exploitation of children, including correspondence and communications between users of child pornography and exploitation websites.

5. Google search terms or Google Maps directions to designated meet location(s);

6. Google search of Undercover Agent ("UCA") phone number or other user names or user accounts of potential minors;
7. Reverse image searches of UCA decoy pictures or pictures of possible minors;
8. Statements regarding awareness of parole conditions;

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high-speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives, flash drives, thumb drives, micro-SD cards, macro-SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.